Biztonság és védelem az informatikában

8. gyakorlati feladat

Készítette: Baranyi Gábor
CRC7FC

2021.04.07.

Personal firewall működési módok

A személyes tűzfal olyan alkalmazás, amely vezérli a hálózati forgalmat a számítógép felé és onnan, engedélyezve vagy megtagadva a kommunikációt a biztonsági irányelvek alapján. Általában alkalmazásréteg-tűzfalként működik.

A személyes tűzfal méretarányosan különbözik a hagyományos tűzfalaktól. A személyes tűzfal általában csak azt a számítógépet védi, amelyre telepítve van, összehasonlítva egy hagyományos tűzfallal, amelyet általában két vagy több hálózat, például útválasztó vagy proxykiszolgáló közötti kijelölt interfészre telepítenek. Ezért a személyes tűzfalak lehetővé teszik a biztonsági házirend meghatározását az egyes számítógépeknél, míg a hagyományos tűzfal vezérli a házirendet az általa összekapcsolt hálózatok között.

A személyes tűzfalak számítógépenkénti hatóköre hasznos a különböző hálózatokon áthelyezett gépek védelmében. Például egy laptop számítógép megbízható intraneten használható egy olyan munkahelyen, ahol minimális védelemre van szükség, mivel a hagyományos tűzfal már működik, és hasznosak a nyitott portokat igénylő szolgáltatások, például a fájlok és a nyomtatók megosztása. Ugyanazt a laptopot lehetne használni a nyilvános Wi-Fi hotspotokon, ahol szükség lehet a bizalom szintjének eldöntésére és a tűzfal beállításainak újrakonfigurálására a számítógép felé irányuló és onnan érkező forgalom korlátozása érdekében. Tűzfal úgy konfigurálható, hogy az egyes hálózatokhoz különböző biztonsági házirendeket engedélyezzen.

A hálózati tűzfalaktól eltérően sok személyes tűzfal képes szabályozni a biztonságos számítógépen lévő programok számára engedélyezett hálózati forgalmat. Amikor egy alkalmazás megpróbál kimenő kapcsolatot létrehozni, a tűzfal blokkolhatja, ha feketelistára kerül, vagy megkérdezi a felhasználót, hogy tegye fel feketelistára, ha még nem ismert. Ez védelmet nyújt a futtatható programként megvalósított rosszindulatú programok ellen. A személyes tűzfalak bizonyos szintű behatolásfelismerést is biztosíthatnak, lehetővé téve a szoftver számára, hogy felszakítsa vagy blokkolja a kapcsolatot, ha gyanítja, hogy behatolásra kerül sor

ELVEK:

Tanuló:

A program automatikusan létrehozza és menti a szabályokat; ez a mód legjobban a tűzfal kezdeti konfigurációjakor használható, állandó használata nem ajánlott. Ebben a folyamatban nincs szükség felhasználói beavatkozásra, mert az ESET Internet Security előre definiált paraméterek szerint menti a szabályokat. A biztonsági kockázatok elkerülése érdekében csak addig tanácsos tanuló módot használni, amíg a program a szükséges kommunikációkhoz létre nem hozza az összes szabályt

Interaktív:

Ez az üzemmód lehetővé teszi a tűzfal egyéni konfigurációjának a kialakítását. Ha a program olyan kommunikációt észlel, amelyhez nincs szabály definiálva, egy párbeszédpanelen jelenti az ismeretlen kapcsolatot. A párbeszédpanelen engedélyezheti vagy letilthatja a kommunikációt, döntését pedig a tűzfal új szabályaként is mentheti. Ha a párbeszédpanelen új szabály létrehozása mellett dönt, a program a szabály alapján az összes hasonló típusú kommunikációt engedélyezi vagy letiltja a jövőben.

Gyakorlati szabályok például:

- a vállalat belső hálózatán levő számítógépek internet felé irányuló valamennyi kapcsolatépítése letiltva, kivéve: a 80-as, kvázi szabvány http porton a vállalat saját weboldalát. Ezt általában elegendő az internetvonal(ak) megosztását (NAT) végző gépen tűzfal szabályként alkalmazni.
- a vállalat belső hálózatán levő számítógépek internet felé irányuló valamennyi kapcsolatépítése letiltva, kivéve: a 80-as http porton és 443-as biztonságos https porton tetszőleges weboldal. Ezt szintén elegendő a NAT-olást végző gép(ek)en tűzfal szabályként alkalmazni.
- a vállalat belső hálózatán levő számítógépek internet felé irányuló valamennyi kapcsolatépítése letiltva, kivéve egyes szolgáltatásokat, mint a http(s), dns, pop3, smtp, egyebek. Ezt a NAT-olást végző számítógépen az egyes szolgáltatásokhoz tartozó kimenő portok engedélyezésével tehetjük meg.
- a vállalat belső hálózatán levő számítógépek egymás közötti hálózati kapcsolatépítésének korlátozása csak engedélyezett szolgáltatásokra: ilyenkor vagy vállalati switchen kell csomagszűrést alkalmazni (például a gépek között mindent letiltunk, kivéve a 137, 138, 139 portokat a fájlmegosztások elérésére), vagy ugyanezt a módszert minden egyes számítógépen alkalmazni kell egy tűzfal programmal.

Tehát honnan tudja, hogy a tűzfala valóban megvéd-e?

Időnként tesztelnie kell a tűzfalat. A tűzfal tesztelésének legjobb módja a hálózaton kívülről (azaz az internetről) származik. Sok ingyenes eszköz áll rendelkezésre ennek megvalósításához. Az egyik legkönnyebben elérhető és leghasznosabb a ShieldsUP a Gibson Research webhelyről. A ShieldsUP lehetővé teszi, hogy több különböző portot és szolgáltatást vizsgáljon a hálózati IP-cím alapján, amelyet a webhely meglátogatásakor fog meghatározni. A ShieldsUP webhelyen négyféle vizsgálat érhető el:

Fájlmegosztási teszt

A fájlmegosztási teszt ellenőrzi a sérülékeny fájlmegosztó portokkal és szolgáltatásokkal társított közös portokat. Ha ezek a portok és szolgáltatások futnak, az azt jelenti, hogy egy rejtett fájlszerver futhat a számítógépén, ami lehetővé teszi a hackerek számára a fájlrendszerhez való hozzáférést

Közös port teszt

A közös portok tesztje megvizsgálja a népszerű (és valószínűleg sérülékeny) szolgáltatások, köztük az FTP, a Telnet, a NetBIOS és sok más által használt portokat. A teszt megmondja, hogy az útválasztó vagy a számítógép lopakodó módja a hirdetések szerint működik-e vagy sem.

Minden port és szolgáltatás teszt

Ez a beolvasás minden egyes portot 0 és 1056 között tesztel, hogy meg vannak-e nyitva (piros színnel jelezve), zárva (kékkel jelezve) vagy lopakodó módban (zöld színnel jelezve). Ha bármelyik portot piros színnel látja, tanulmányozza tovább, hogy mi fut ezeken a portokon. Ellenőrizze a tűzfal beállításait, hogy ezeket a portokat valamilyen konkrét célra adták-e hozzá.

Ha nem lát semmit a tűzfalszabálylistában ezekről a portokról, az azt jelezheti, hogy rosszindulatú program fut a számítógépén, és lehetséges, hogy a számítógépe egy botnet részévé vált. Ha valami zavarosnak tűnik, akkor

használjon anti-malware szkennert, hogy ellenőrizze a számítógépét, hogy vannak-e rejtett kártékony programok

Messenger spam teszt

A Messenger Spam teszt megpróbálja elküldeni a Microsoft Windows Messenger tesztüzenetét a számítógépére, hogy lássa, a tűzfala blokkolja-e ezt a szolgáltatást, amelyet a spammerek kihasználhatnak és felhasználhatnak üzenetek küldésére. Ez a teszt csak a Microsoft Windows felhasználók számára készült. A Mac / Linux felhasználók kihagyhatják ezt a tesztet.

Böngésző közzétételi teszt

Bár nem tűzfalpróba, ez a teszt megmutatja, hogy a böngésző milyen információkat árulhat el rólad és a rendszeréről.

A tesztek során remélhető legjobb eredmény az, ha elmondja, hogy számítógépe „True Stealth" módban van, és a vizsgálat során kiderül, hogy a rendszerén nincsenek olyan nyitott portok, amelyek az internetről láthatóak / elérhetők lennének. Miután ezt elérte, kissé könnyebben alhat, tudván, hogy a számítógépe nem tart nagy virtuális jelet, amely "Hé! Kérem, támadjon meg!"

Legjobb 5 tűzfal:

1. McAfee LiveSafe

Ár: 104,99 USD / év, korlátlan mennyiségű eszközért

Elérhető: Mac és Windows rendszereken

A McAfee LiveSafe egy víruskereső szoftver, amely megvédi számítógépét a vírusoktól és a ransomware-től.

2. Norton Security Premium

Ár: 54,99 USD / év legfeljebb öt eszközért

Elérhető: Mac és Windows rendszereken

A Norton Security Deluxe az egyik legnagyobb polgári cyber hírszerző hálózatot használja fel, hogy megvédje számítógépét a vírusoktól, kémprogramoktól, rosszindulatú programoktól, ransomware-től és más fejlett online fenyegetésektől.

3. Kaspersky Internet Security

Ár: 47,99 USD / év legfeljebb három eszközért

Elérhető: Mac és Windows rendszereken

Amellett, hogy megvédi számítógépét a vírusoktól, a ransomware-től és az internetes támadásoktól, amikor az interneten böngészik vagy bármit letölt, a Kaspersky Internet Security megvédheti bankja és kártyájának adatait is, amikor online bankol vagy vásárol, és megóvja személyes adatait a közösségi oldalakon található rosszindulatú linkektől.

4. Intego Mac Premium Bundle X9

Ár: 69,99 / év legfeljebb három eszközhöz

Elérhető: Mac

Az Intego Mac Premium Bundle legújabb verziójának megvásárlása és letöltése után felhasználhatja a valós idejű víruskereső szoftvert, amely automatikusan átvizsgálja a Mac számítógépét, valamint egy intelligens tűzfalat és egy hotspot hálózati védelmi eszközt, amely megakadályozza a számítógépes bűnözőket abban, hogy az interneten keresztül hozzáférjenek a számítógépéhez.

5. Bitdefender Internet Security

Ár: Évente 79,99 USD legfeljebb három eszközért

Elérhető: PC-n

Azáltal, hogy folyamatosan tesztelte a különféle típusú védelmet a rosszindulatú programok észlelésében, független laboratóriumok által, a Bitdefender Internet Security eléggé kifinomította megoldásaikat, hogy a legjobb internetes támadások megelőzését, ransomware-védelmet, valós idejű adatvédelmet, csalásellenes és adathalász eszközök. Emellett hozzáférést kínálnak saját VPN-jükhöz, a webkamerák védelméhez és a sebezhetőségi felmérésekhez.

Személyes vélemény:

Személyes 1. Windows Defender

Ár:Ingyenes

Elérhető:Windows

Szerintem a legjobb a windows defender és nem kell költeni semmilyen vírusirtóra vagy personal firewall-ra.

Források:

https://en.wikipedia.org/wiki/Personal_firewall

https://www.lifewire.com/how-to-test-your-firewall-2487969#so-how-do-you-know-if-your-firewall-is-actually-protecting-you

https://hu.wikipedia.org/wiki/T%C5%B1zfal_(sz%C3%A1m%C3%ADt%C3%A1stechnika)

https://blog.hubspot.com/marketing/personal-firewall